Commercial and Internet Trends and the NASA Spaceflight Ground Network

M. Chris Spinolo
NASA, Goddard Space Flight Center
Code 291
Greenbelt, MD 20771
301-286-7552
chris.spinolo@gsfc.nasa.gov

Abstract—[1]NASA is a critical information source in this Age of Information. With the advent and maturity of the Internet, the demand for NASA information has grown beyond science data archives to near real time and even real time data, particularly on the Earth and near Earth ecosystems. NASA also has prospered a policy of sharing mission responsibility with non-NASA entities, which still require tracking support from the NASA network. This paper discusses the issues in conflict when trying to solve the paradox of securing a critical national resource and participating as a good citizen of the Information Age. By illustrating several ground network architecture examples, these issues are highlighted. Recommendations for using the NASA tracking networks are given.

TABLE OF CONTENTS

1. INTRODUCTION

The NASA spaceflight tracking[1] and supporting ground networks[2] are critical national resources protected under federal statute, requiring thorough IT security measures. However, it is no longer the only spaceflight game in town. Commercial spacecraft tracking networks and flight operations have followed commercial launch service availability and are now a viable option for spaceflight programs.

The ubiquity of the Internet continues to increase day to day, spawning an increasingly insatiable appetite for information; and the more current the information, the more demand there is for it. Some of the most useful information, for casual, commercial and critical users, is space and terrestrial environmental data[3] gathered from NASA programs.

These two trends have created a growing conflict in requirements for the NASA tracking network, between protection of a critical national resource and delivering program products to the customer and public. Through the use of various ground network architecture examples, the issues and solutions are illustrated. The approach is pragmatic; the perspective that of a network operator who has dealt with and successfully served dozens of diverse spaceflight programs.

2. CURRENT TRENDS - CONFLICTING ISSUES

NASA Tracking Networks Security Posture

As the Federal Government oversight bureaus (i.e. Inspector General, FBI) become more aware of information technology (IT) security risks and issues[4], NASA IT resources come under increasing scrutiny and evaluation. As a result, security postures and measures continue to grow more stringent and pervasive. Many policies that were accepted only a year ago are now seen to be unacceptable risks. However the architectural approach at the highest level remains intact. NASA Resources are categorized as "closed" or "open". Closed resources are those deemed sensitive enough to require a high degree of isolation because of performance requirements or criticality of the resource (e.g. compromise may result in catastrophic loss of life or property). Open resources are those not classified as closed. Data can be passed between a closed network resource and any open network resource only by a single, NASA operated secure gateway facility. The NASA tracking network is a closed resource. Most of the NASA spacecraft control centers are still closed resources.

[1] U.S. Government work not protected by U.S. Copyright.

However current outsourcing trends have customers of the data the NASA tracking network acquires as open resources.

Commercial tracking networks[5]

Several years ago, NASA spun off the launch services it had developed so that a program no longer approaches NASA for a launch service but acquired this service directly from the commercial market place. Even NASA purchases these launch services now. Recently, NASA has prospered a policy to commercialize tracking network services as well. Already several startup commercial tracking networks have been established, which offer spacecraft tracking service on a per pass basis. NASA programs are encouraged to use them, and they are attractive for cost reduction. The challenge for the network, in this scenario, is to provide data delivery to closed NASA resources (mission control centers) while protecting the entire closed network from what is essentially an Internet based service offering.

Outsourced flight operations

As the aerospace industry has matured and proliferated, the opportunity to commercialize flight operations is an attractive option. While NASA science programs are still established and managed by the Administration, universities and aerospace companies now propose to establish and run their own mission operations and control center, rather than rely on government furnished facilities and systems. These external control centers are open resources that still require support from the closed NASA tracking network.

Realtime Customers

The application of NASA, space based technology and information in a way that directly enhances the quality of life here on earth is a strategic goal of the agency. For example, the use of real time data from an outpost between the sun and earth provides early warning of solar eruptions that would be damaging to systems that provide a critical support infrastructure for life on the surface. This early warning capability also increases the safety margin for space explorers working on the space station. Another example is a new mission, currently underway, to provide constant, near realtime views of the earth with the explicit goal of prospering a global perspective among the public, in order to foster cooperation and compassion among otherwise diverse peoples. These mission concepts require a capability to constantly deliver realtime data from the closed NASA tracking networks to the public Internet

3. Configuration Examples

What follows are descriptions of various attempts to build ground support networks for flight projects and the risks assumed by each particular architecture.

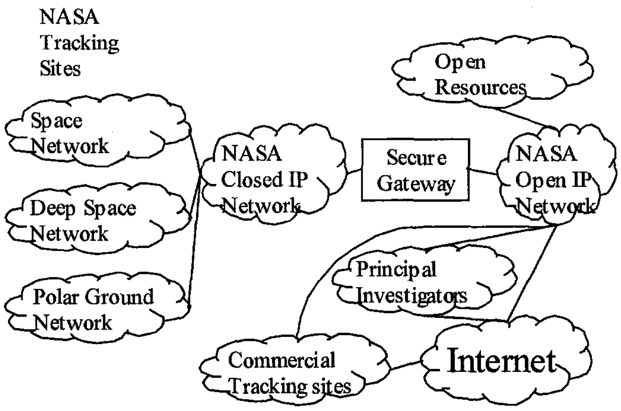

Figure 1. Conceptual Drawing

Figure 1 illustrates a conceptual diagram of the relationship between the various components discussed in this paper. The most significant feature is the isolation of mission critical resources in the closed side of the network. Security policies dictate that no resources are allowed to be connected to the closed network and any other network. This is commonly referred to as an “air gap” security posture, and has never been waived by NASA. The “customer” Science operations and principal investigators have always been, and continue to be open resources. Other pertinent features are:

- Access to the closed network is only possible via the single, NASA owned secure gateway.
- Connections through the secure gateway must be initiated from the closed network, no connections are initiated from the open network to the closed network resources.
- Encrypted data flows are not permitted through the secure gateway.
- Network performance levels are specified and delivered effectively by the closed network. Such guarantees are not perceived to be possible in an open network where network use is not controlled.

A ground system architecture is determined by analyzing the mission operations concepts to determine the primary tracking network, placement of the control center and other critical real time resources in relation to the tracking network, placement of science operations and principal investigators, and providing a delivery mechanism for mission products to the customer and public.

Closed Example

This scenario (Figure 2) is typical of the majority of existing NASA missions. The control centers are located at NASA sites and connected to the closed network. The most significant advantage of this configuration is the fault tolerant, highly available connectivity between the control center and the tracking stations. Another advantage of this approach is the simplicity of the security plan for critical facilities, which take advantage of the isolation of the NASA closed network. The primary disadvantage is the elimination of connectivity options for the control center which now has only one door behind NASA's secure gateway. Initially this may seem significant, but as launch approaches and critical support actually comes in view, most programs take level of comfort in this architecture. The comfort level comes from the self control and validated rules of engagement enforced by connection to the closed network, not just the "protection" (real or perceived) afforded by features such as the secure gateway.

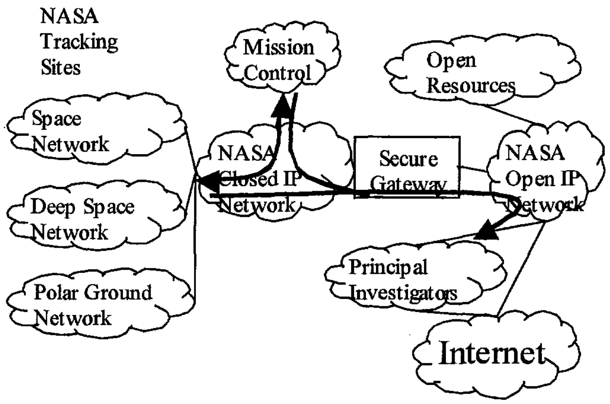

Figure 2. Closed Mission Ops Data Flows

The control center can also be located at a university or commercial facility in this mission architecture, but must be strictly isolated from any other network. While feasible, many mission concepts with non- NASA control centers rely on existing resources at the university or corporation for cost savings, making such isolation problematic.

This is the recommended configuration for a mission that relies on the NASA Tracking network as the primary tracking network.

Open Example

In this mission architecture, the entire operation, with the exception of the actual spacecraft tracking, is in the open network. The primary advantage, indeed the chief goal of this approach, is to allow the project maximum flexibility in distributing and collaborating with 3rd party participants. The primary disadvantage is the risk of separation from the NASA tracking stations inherent in the secure gateway. Another feature, which could be pro or con, is the responsibility for IT security of the control center rests solely with the project.

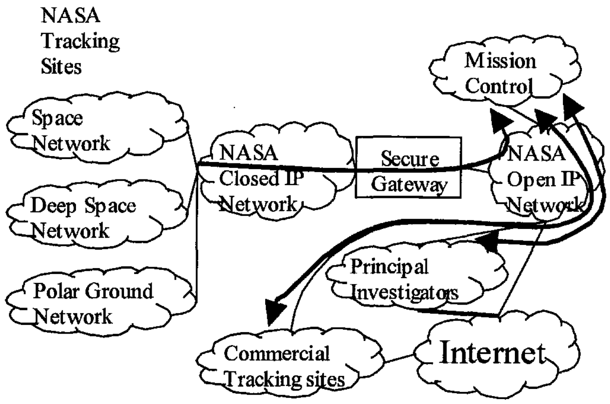

Figure 3. Open MOC Data Flows

This is the recommended architecture for missions that will use commercial tracking services as the primary tracking network. It is highly likely that such missions will still rely on NASA tracking networks for launch, early mission coverage and contingency support. Even though these data flows are 2-way, these connections must be initiated from the closed network.

Commercial Tracking and Operations

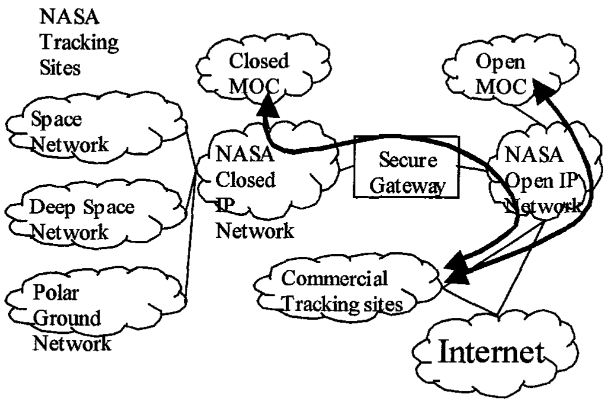

Figure 4. Commercial Tracking Services

The last conceptual example highlights a new issue created with the advent of commercial tracking networks. With this new service offering, new and existing NASA missions can purchase pass support "off the market." This requires that realtime support be configured from an open resource to a Mission control (MOC) center on the closed network. These data flows must be initiated from the control center. The passes are usually scheduled via an Internet interface, so the closed MOC also requires direct connections to the open side, but entirely isolated from the closed segments. This issue has resulted in some new mission choosing to locate the control center on the open network (see Open Example)

The method for securing the data flows between the commercial tracking networks and the control centers is still to be determined. Federal law requires that the command uplink to federally and NASA sponsored satellites be protected, including the ground segment. This risk is presently mitigated by dedicated IP connections (e.g. not Internet) to the commercial provider.

Summary

The key considerations for projects considering the use of NASA tracking networks in their mission profile are:

- The NASA tracking network is an isolated secured facility with established and enforced access policies. This provides an infrastructure for highly available, safe access between the spacecraft and the control centers.
- U.S. Government law and policy requires significant security practices for spacecraft projects and audit the projects to check compliance. These policies are becoming more restrictive and less flexible, even in light of emerging technologies conflicting program policy.
- There is a trade off between access to the spacecraft through the NASA tracking network and access to the Internet and other networks for product distribution and project collaboration.

4. Working Successes

This section describes actual online successes.

ACE

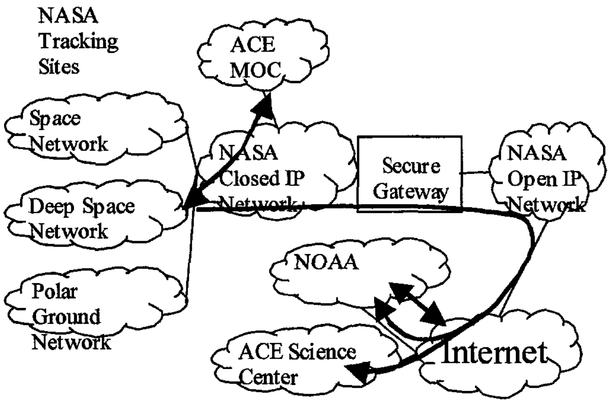

Figure 5. ACE Mission

The Advanced Composition Explorer[6] (ACE) is the first NASA mission to use IP as the ground transport mechanism, and is one of the most successful. This mission architecture has proven to be robust, secure and very flexible.

The major characteristics of this mission architecture are the closed MOC, open science operations center (SOC, where the spacecraft instruments are managed) and a constant realtime customer, NOAA, who provides early warning capability of damaging solar eruptions to the public[7]. All connections from the closed to the open networks must be initiated from the closed side. In order for NOAA to receive spacecraft data when the MOC is not in contact with the through the Deep Space Network, they have scheduled tracking time on the U.S. Air Force and various foreign research facilities in Japan, U.K. and India.

All critical segments of the ground system reside in the closed network where they enjoy high network availability and isolation. All spacecraft commanding is done from the MOC.

Landsat 7

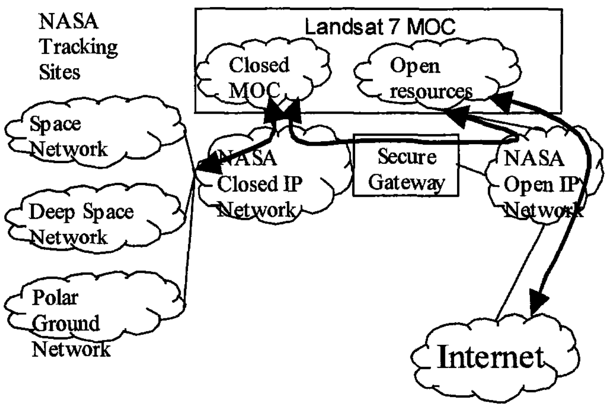

Figure 6. Landsat 7

The Landsat 7 ground system architecture is similar to ACE, but has positioned itself for greater flexibility toward the Internet by implementing an open side connection in the MOC. This approach is very attractive to the secure gateway since all connection requests are between system managed by the MOC and remain very static, i.e., the secure gateway rules do not have Internet addresses. The mission operations concept can now freely add support to customers in the Internet. There is an assumption, and requirement for, a system administrator in the MOC with heightened security awareness and savvy. A compromise in the open MOC resources may provide access to the closed MOC through valid secure gateway rules.

Remote Control Centers

Several missions, including most of the new, emerging missions, have control centers that are not NASA operated or located. These new missions also plan to take advantage of emerging commercial tracking services.

The important points of consideration in this configuration are that the connections from the NASA tracking networks must be initiated from the closed side and the project has a larger role in securing the critical MOC from the Internet. This configuration gives the project considerable autonomy in regard to its ground network architecture, policy and mission concepts.

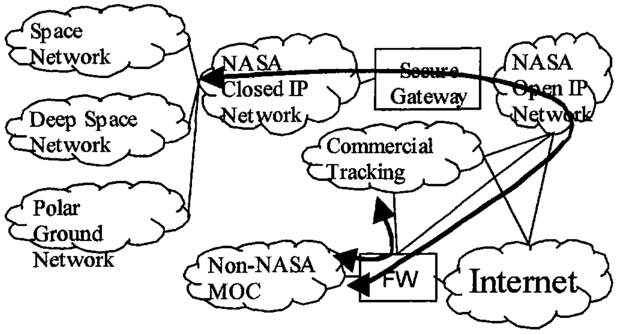

Figure 7. NASA Outsourced Control Centers

This configuration is becoming the most common among the emerging missions as NASA promotes the "commercialization" of more segments of the space program. The main concern here is the proper and adequate application of significant security measures such that the NASA mission satisfies law and policy, and is not put at inordinate risk.

TRIANA

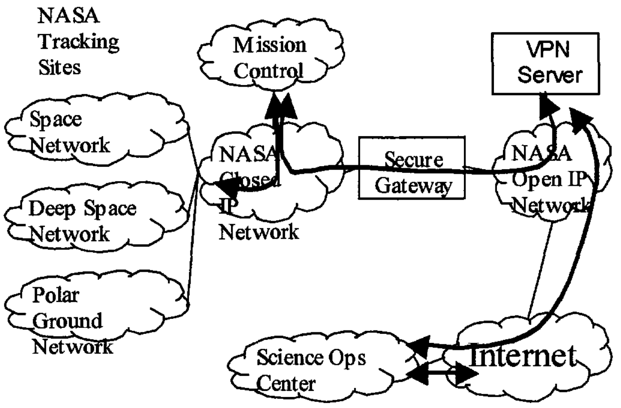

Figure 8. Triana

The Triana mission[8] (to be launched in 2002) is interesting because of the use of encryption in a portion of the ground system.

Background – The Triana mission is to orbit a satellite at L1, between the earth and sun, providing a continuously updated global view of the earth for the Internet, and other science objectives.

The Triana ground system can be separated into two major parts, the mission operations segment, responsible for the operation and safety of the actual spacecraft, and the science operations which manages and delivers the mission products. The mission side is entirely closed and located at a NASA facility while the science side is on the open side and located at a university in California. Because the SOC will actually generate command loads for the spacecraft, the data must be secured as it traverses the Internet. Thus the data is transmitted over a virtual private network through the Internet which provides encryption and privacy.

Encrypted data flows are not permitted by the network security plan, through the secure gateway. This restriction is required to permit visibility at the secure gateway to verify compliance and proper use. Therefore the encrypted path over the Internet ends in a NASA operated subnet on the open side of the secure gateway.

VPN Caution – Encryption must be used in a circumspect way, and should not be considered a generalized cure for security issues, it is only a piece of the solution, a tool at our disposal. A common failure in the execution of many security plans happens when the implementation of "neat" technology causes the project to lower its guard and lose its IT security vigilance, particularly at the host level. The result is a system compromise allowing encrypted access into the critical segment of the ground system. This is possible because VPNs imply trusted hosts, and trusted hosts are a loophole of many an IT security plan.

5. CONCLUSIONS

The NASA tracking networks are a valuable national resource and many aerospace programs use the network as part of its mission operations concepts. The network is implemented to provide extreme availability and safety for its users, but in order to accomplish its mission, access policies are strict and enforced. Missions that use the NASA tracking network as the primary spacecraft tracking network should consider these issues carefully and early so that they are compatible with the closed network. As more of the aerospace mission concepts becomes more commercialized, they must still comply with established government policies[9].

Trends that bring the public at large into the mission operations concept, and the application of Internet technology to the aerospace disciplines (e.g. the spacecraft as an IP node) expose the mission to an ever greater risk. As their exposure increases spacecraft will become popular targets of hacker opportunity.[10] The aerospace community must stay at the forefront of IT security technology.[11]

REREFENCES

[1] Space Network
http://msp.gsfc.nasa.gov/tdrss/

[2] The NASA IP Operational Network
http://forbin2.gsfc.nasa.gov/prodserv/IONET/ionet.stm

[3] Examples on online terrestrial information
http://seawifs.gsfc.nasa.gov/SEAWIFS.html
http://www.earthwatch.com/SKYWATCH/skywatch.html

[4] NASA Policies and Guidelines
http://nodis.gsfc.nasa.gov:80/Library/Directives/NASA-WIDE/Procedures/Legal_Policies/N_PG_2810_1.html

[5] The Universal Space Network
http://www.uspacenetwork.com/

[5] AlliedSignal is a developing a new satellite command, control and communications network, DataLynx
http://www.alliedsignalaerospace.com:80/aerospace/services/datalynx/index.html

[6] Advanced Composition Explorer Homepage
http://helios.gsfc.nasa.gov/ace/ace.html

[7] ACE Real Time Solar Wind
http://sec.noaa.gov/ace/

[8] The Triana homepage
http://triana.gsfc.nasa.gov/home/

[9] IT contractors must follow NASA security rules
http://www.fcw.com/fcw/articles/2000/0717/web-nasa-07-17-00.asp

[10] IP on the Spacecraft
http://www.newscientist.com/news/news_224641.html

[11] Other good IT security references:
Internet Engineering Task Force User Security Handbook (RFC2504)
http://www.ietf.org/rfc/rfc2504.txt?number=2504

[11] Internet Engineering Task Force Site Security Handbook (RFC2196)
http://www.ietf.org/rfc/rfc2196.txt?number=2196

[11] The Common Criteria (ISO IS 15408) is a structured way of evaluating the security requirements and properties of a product or system.
http://niap.nist.gov/cc-scheme/

[11] The Computer Security Technology Center, located at the Lawrence Livermore National Laboratory
http://www.ciac.org/cstc/

[11] Good security web site.
http://www.securityfocus.com/

__Chris Spinolo__ is the Lead Engineer for the NASA IP Operational Network. The IONet is the mission critical, real time, ground segment network for all NASA manned and unmanned space flights, from the Space Shuttle and Hubble Space Telescope, to high altitude balloon flights. This world wide, mission critical network connects NASA and other tracking stations with dozens of mission control centers throughout the world.